UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- x

UNITED STATES OF AMERICA	:	SEALED INDICTMENT
- v. -	:	S2 11 Cr. 878
VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV,	:	
Defendants.	:	

- x

COUNT ONE

(Conspiracy to Commit Wire Fraud)

The Grand Jury charges:

Overview of the Scheme

1. From at least in or about 2007, up to and including in or about October 2011, in the Southern District of New York and elsewhere, VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants (collectively, "the defendants"), and others known and unknown, engaged in a massive and sophisticated scheme that infected at least four million computers located in over 100 countries with malicious software, or "malware."[1] Without the

[1] Attached as Exhibit A is a glossary of computer-related terminology used in this Indictment.

computer users' knowledge or permission, the malware digitally hijacked the infected computers to facilitate the defendants' commission of Internet advertising fraud, as described below. Victims' computers were infected with the malware when, among other means, their computers visited certain websites, or when victims downloaded certain software from websites including, but not limited to, software that enabled victims to view videos online.

2. The defendants and their co-conspirators operated and controlled companies that masqueraded as legitimate participants in the Internet advertising industry. Through those companies, the defendants and their co-conspirators entered into agreements under which they would be paid based upon the number of times that Internet users "clicked" on the links for certain advertisements, or based upon the number of times that certain advertisements were displayed on certain websites. Rather than earn money legitimately under those agreements, the defendants and their co-conspirators instead devised a criminal scheme to infect millions of computers (the "infected computers") with malware that surreptitiously redirected those computers to the websites and advertisements that would generate illicit advertising revenue for the defendants. As described below, components of this advertising fraud scheme included what this Indictment refers to as (i) "click hijacking fraud"; and (ii) "advertising replacement fraud." Moreover, in

order to protect the scheme from being thwarted, the malware used by the defendants and their co-conspirators was designed to prevent the installation of anti-virus software updates - leaving the infected computers, and their users, unable to detect or stop the defendant's malware, and vulnerable to other malware.

The Click Hijacking Fraud

3. One component of the defendants' fraud scheme involved click hijacking. When the user of an infected computer clicked on a search result link displayed through a search engine query, instead of being brought to the website to which the user asked to go, the malware caused the computer to be re-routed to a different website designated by the defendants, so as to trigger payment to the defendants under one or more advertising contracts. This click hijacking occurred for clicks on so-called "organic" search results as well as clicks on "sponsored" links.[2] Examples of how the click hijacking fraud worked include the following:

a. **The Apples-iTunes Example.** Attached as Exhibit B is an illustration of how the user of an infected computer clicked on a link for the official Apple-iTunes website, but was

---

[2] "Organic" search results are the unpaid links that appear in response to a user's search query. "Sponsored" links are, in essence, advertisements that appear in response to a user's search query - often at the top of or to the right of organic search results. Search engines typically receive money, on a per-click basis, when a sponsored link is clicked by a user.

instead taken to a different website. As Exhibit B illustrates, using the Google search engine, the user searched for the term "itunes." The search results displayed a number of links, the very first being a purported link to "www.apple.com/itunes/" - which is, in fact, the domain name for the official iTunes website maintained by Apple, Inc. The user of the infected computer then clicked on that link, but instead of being taken to that website, the link - by the defendants' design - opened a website for www.idownload-store-music.com, which is a business unaffiliated with Apple Inc., that purported to sell Apple software. The defendants then received money for that fraudulently engineered "click."

b. **The Netflix Example.** Attached as Exhibit C is an illustration of how the user of an infected computer clicked on a link for Netflix, but was instead taken to the website for an unrelated business called "BudgetMatch." As Exhibit C illustrates, using the Bing search engine, the user searched for the term "netflix." The search results displayed a number of links, including a purported link to "www.netflix.com " - which is, in fact, the domain name for the official website of Netflix, a movie rental business. The user of the infected computer then clicked on that link, but instead of being taken to that website, the link - by the defendants' design - opened a website for www.budgetmatch.net, which

is not affiliated with Netflix. The defendants then received money for that fraudulently engineered "click."

c. **The Internal Revenue Service Example.**

Attached as Exhibit D is an illustration of how the user of an infected computer clicked on a link for the Internal Revenue Service, but was instead taken to the website for a major tax preparation business. As Exhibit D illustrates, using the Yahoo search engine, the user searched for the term "irs." The search results displayed a number of links, the first being a purported link to "www.irs.gov " - which is, in fact, the domain name for the website of the Internal Revenue Service. The user of the infected computer then clicked on that link, but instead of being taken to that website, the link - by the defendants' design - opened a website for H&R Block (www.hrblock.com), which is not affiliated with the IRS. The defendants then received money for that fraudulently engineered "click."

The Advertising Replacement Fraud

4. Another component of the defendants' fraud scheme involved advertising replacement fraud. In this component of the scheme, the defendants and their co-conspirators replaced legitimate advertisements on websites with substituted advertisements that triggered payments to the defendants. Examples of how the advertising replacement fraud worked include the following:

a. **The Wall Street Journal Example.** Attached as Exhibit E are side-by-side screenshots of the publication of the Wall Street Journal ("WSJ") website's home-page on May 31, 2010. Both screenshots were obtained by using a computer's web browser to go to "http://online.wsj.com/home-page." The screenshot on the left was obtained from a non-infected computer, whereas the screenshot on the right was obtained from an infected computer. On the non-infected computer, the WSJ home-page prominently displayed an advertisement (in the lower right hand side of the webpage) for American Express, advertising "The Plum Card." On the infected computer, that advertisement had been replaced - by the defendants' design - with an advertisement for "Fashion Girl LA."

b. **The Amazon.com Example.** Attached as Exhibit F are side-by-side screenshots of the Amazon.com website. The screenshot on the left was obtained from a non-infected computer, whereas the screenshot on the right was obtained from an infected computer. On the non-infected computer, a prominent advertisement was displayed on the lower right hand side of the webpage for Windows Internet Explorer8. On the infected computer, that advertisement had been replaced with an advertisement - by the defendants' design - for an email marketing business.

c. **The ESPN Example.** Attached as Exhibit G are side-by-side screenshots of the ESPN website. The screenshot on the

left was obtained from a non-infected computer, whereas the screenshot on the right was obtained from an infected computer. On the non-infected computer, prominent advertisements for Dr. Pepper, a soft-drink, were displayed on ESPN's webpage. On the infected computer, the Dr. Pepper advertisements had been replaced - by the defendants' design - with an advertisement for a timeshare business.

5. As a result of this scheme, VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, and their co-conspirators, reaped at least $14 million in ill-gotten gains through click hijacking and advertisement replacement fraud. Of the more than four million computers infected with malware as a part of the scheme, at least 500,000 were infected computers in the United States, among them computers belonging to United States government agencies, such as the National Aeronautics and Space Administration ("NASA"); educational institutions; non-profit organizations; commercial businesses; and individuals.

The Blocking of Anti-Virus Software

6. As a further part of the scheme, and to prevent its detection, VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, and their co-conspirators, designed the malware to disable anti-virus protections on the infected computers.

Specifically, the malware prevented anti-virus software on the infected computers, as well as security features of the infected computers' operating systems, from receiving updates that otherwise could have detected the malware and stopped it. As a result, the infected computers were left vulnerable to infections by malware distributed by other cybercriminals which could, among other harms, steal the computers users' valuable personal and financial information.

7. Attached as Exhibit H are screenshots showing what occurred when the user of an infected computer tried to access websites that host anti-virus and/or operating system updates. An attempt to access a Microsoft operating system update from an infected computer resulted in the message: "The page cannot be displayed. The page you are looking for is currently unavailable." An attempt to access Avast! anti-virus software resulted in the message: "Error: Cannot connect to server." An attempt to access AVG anti-virus software resulted in the message: "Connection failed." Accordingly, the defendants' scheme – in addition to harming computer users by hijacking computer searches and bringing users to websites and advertisements they never intended to visit – further harmed computer users by disabling their anti-virus software protections and leaving their computers vulnerable to other malware.

8. The defendants' scheme also deprived legitimate website operators and advertisers of substantial monies and advertising revenue. Search engines lost revenues as a result of the hijacking of clicks on their sponsored search results listings. Advertisers lost money by paying for clicks that they believed to be bona fide clicks by interested computer users, but which were in fact fraudulently engineered by the defendants. Furthermore, the defendants' conduct risked reputational harm to businesses that paid to advertise on the Internet - but that had no knowledge or desire for computer users to be directed to their websites or advertisements through the fraudulent means used by the defendants.

The Defendants and Relevant Entities

9. At all times relevant to this Indictment, VLADIMIR TSASTSIN, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, were Estonian nationals residing in Estonia.

10. At all times relevant to this Indictment, ANDREY TAAME, the defendant, was a Russian national residing in Russia.

11. At various times relevant to this Indictment, VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, and their co-conspirators, operated and controlled entities used to execute the fraudulent advertising scheme and to

launder the illicit profits from it, including the following companies, among others:

a. Rove Digital, an Estonian corporation, which was purportedly in the business of, among other things, software development;

b. Tamme Arendus, an Estonian corporation, which purportedly was a real estate development business and which acquired most of Rove Digital's assets;

c. SPB Group, the entity name under which TSASTSIN and his co-conspirators rented from a data center in New York, New York (the "Manhattan Data Center") several servers and other technology infrastructure that enabled the click hijacking and advertising replacement frauds;

d. Cernel Inc., a California company ("Cernel"), Internet Path Limited, a New York company ("Internet Path"), Promnet Limited, a Ukrainian company ("Promnet"), ProLite Limited, a Russian company ("ProLite"), and Front Communications, a New York company ("Front"), which were used to register thousands of IP addresses assigned to the defendants' computers in furtherance of the fraud scheme;

e. Furox Aps, d/b/a "Gathi.com," a Danish company ("Furox"), Onwa Limited, d/b/a "UtterSearch.com" ("Onwa"), a Republic of Seychelles company, and Lintor Limited, d/b/a

"Crossnets.com," a British company ("Lintor"), that entered into agreements with advertising brokers to deliver Internet traffic, as discussed below; and

f. IT Consulting, Infradata, and Novatech, all Estonian companies, which, along with Rove Digital, Furox and Onwa, maintained accounts in Cyprus, Denmark and Estonia, among other places, that received millions of dollars in advertising fees derived from the fraudulent advertising scheme.

Internet Advertising

12. Internet advertising is a multi-billion dollar industry in which website owners sell advertising space on their websites. Two common advertising arrangements are the so-called "pay per click" model and the "pay per impression" model. Under either arrangement, a website operator (also referred to as a "publisher") contracts with an advertiser to display an advertisement on the website.

13. Under the "pay per click" model, and in its simplest form, the advertiser pays the publisher a certain amount of money each time a visitor to the website clicks on a particular advertisement and is sent to another website which provides the visitor with additional information about the advertised product or service.

14. Under the "pay per impression model," and in its simplest form, the advertiser pays the publisher a certain amount of money each time an advertisement is displayed on a webpage that is viewed, but not necessarily clicked on, by a visitor.

15. There are millions of website publishers and advertisers on the Internet. As a result, instead of having a direct relationship with a website publisher, advertisers often rely on third-party "ad brokers" to contract with and deliver their advertisements to website publishers. Similarly, rather than contract with ad brokers individually, website publishers often join together to form "publisher networks" to contract with ad brokers collectively.

16. Internet advertisements appearing on websites pursuant to such contracts are digitally "tagged." Thus, when a user views or clicks on an advertisement, the appropriate ad broker which distributed the ad and the website publisher network which displayed the ad can be identified, and payment can be remitted to them.

The Defendants' Scheme to Commit Advertising Fraud Through their Operation of Publisher Networks

17. From at least in or about 2007, up to and including in or about October 2011, the defendants controlled and operated various companies which purported to be legitimate publisher networks, including but not limited to Furox, Onwa, and Lintor

(collectively, "the Defendants' Publisher Networks"). Those Publisher Networks entered into advertising agreements with multiple ad brokers, giving the defendants a financial motive to maximize the number of clicks on the advertiser websites, and the number of ad displays, attributable to the Defendants' Publisher Networks. Stated another way, the more Internet traffic that the Defendants' Publisher Networks drove to the advertisers' websites and display ads, the more money the defendants would earn under their agreements with the ad brokers.

18. In truth and in fact, however, and as VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, well knew, most, if not all, of the websites that purported to be part of the Defendants' Publisher Networks were bogus websites controlled by the defendants to enable a massive fraud.

19. The defendants "earned" millions of dollars under their advertising agreements, not by legitimately displaying advertisements through their Publisher Networks, but instead by using malware to fraudulently drive Internet traffic to certain advertiser websites and display ads. Furthermore, the defendants took steps to make it appear to advertisers that this traffic was from legitimate clicks and ad displays originating from the Defendants' Publisher Networks and their member websites.

The Defendants' Use of "Rogue DNS Servers" and "DNS Changer Malware" to Execute the Scheme

20. To carry out the scheme, VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, and their co-conspirators used what are known as "rogue" Domain Name System ("DNS") servers, and malware that was designed to alter the DNS server settings on infected computers (the "DNS Changer Malware"), as described below.

21. By way of background, a computer user can access a website on the Internet by either of two principal ways: by entering into the computer's web browser either the Internet Protocol ("IP") address, or the domain name, for that website. The IP address is a unique numerical address associated with a website (e.g., 123.45.6.78), akin to a home or business street address; whereas a domain name is a simple, easy-to-remember way for humans to identify computers on the Internet (such as "www.irs.gov").

22. When a computer seeks to access a website by its domain name, it uses a DNS server to first convert or "resolve" the domain name into the IP address for that website. The computer's internet service provider ("ISP") typically transmits the IP addresses for one or more legitimate DNS servers operated by the ISP, and that information is stored in the computer's operating system.

(The DNS settings of a user's computer also can be changed without the user's permission by malware.) After the computer receives the IP address from a DNS server, it then uses that IP address to find the requested website and retrieve and display the relevant webpages.

23. Using the IRS website to illustrate how a DNS server works, if a computer user entered the domain name "www.irs.gov" into the computer's web browser, the web browser would first refer to the DNS server as directed by the computer's operating system; then contact the DNS Server to obtain the IP address corresponding to www.irs.gov; and then use the IP address to locate the computer connected to the Internet that hosts the www.irs.gov website and, ultimately, to retrieve and display that website for the user.

24. DNS servers are thus critical to the proper functioning of the Internet. Computer users rely on DNS servers to correctly resolve domain names so that the users' computers receive the correct IP address information and so that, accordingly, users access the websites they intended.

25. A "rogue" DNS server is a DNS server that intentionally resolves a domain name to an incorrect IP address, and therefore directs a computer user to an incorrect website.

26. Here, in furtherance of the scheme, VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, and

their co-conspirators, controlled and operated dozens of rogue DNS servers (the "Rogue DNS Servers") located in, among other places, New York, New York and Chicago, Illinois.

27. As a further part of the scheme, the defendants and their co-conspirators distributed the DNS Changer Malware that was designed to alter the DNS server settings on victims' computers, to route the infected computers to Rogue DNS Servers, instead of legitimate DNS servers. Specifically, the DNS Changer Malware altered the DNS server IP addresses stored in the infected computers' operating systems to the IP addresses of the Rogue DNS Servers controlled and operated by the defendants and their co-conspirators. Among other means, the DNS Changer Malware infected the victims' computers when those computers visited certain websites, or when victims downloaded certain software from websites including, but not limited to, software that enabled victims to view videos online.

28. The defendants and their co-conspirators then caused the Rogue DNS Servers that they controlled and operated to divert users of the infected computers to websites and advertisements that the users did not intend to visit, but for which the defendants and their co-conspirators received fees based on the Internet traffic agreements between the Defendants' Publisher Networks and the ad brokers.

29. Thus, to carry out the click hijacking fraud, using the IRS example discussed in paragraph 3(c) above, when the user of an infected computer conducted a Yahoo search for "irs," the infected computer first contacted one of the Rogue DNS Servers for the IP address of Yahoo's search results webpage. Instead of returning the IP address of the true Yahoo search results webpage, the Rogue DNS Server instead returned the IP address of a fraudulent, imitation webpage created by the defendants to resemble the legitimate Yahoo search results webpage. When the computer user then clicked on a link to a result on this imitation Yahoo webpage, the click was "hijacked" by the defendants and their co-conspirators who instead diverted the user to a different website of the defendants' and their co-conspirators' choosing, for which they "earned" advertising revenue.

30. Similarly, to carry out the advertising replacement fraud, the defendants and their co-conspirators caused the Rogue DNS Servers to display alternate advertisements on certain websites when the users of infected computers viewed those websites using a web browser. When the web browser executed the links associated with a particular advertising banner, in order to display that advertisement, the Rogue DNS Servers resolved the domain names in those links to IP addresses of computers hosting the substitute advertisements.

31. As a further part of the scheme, and to ensure that they were paid advertising fees by ad brokers, the defendants and their co-conspirators caused information relating to a particular hijacked click or substitute advertisement to be manipulated to make it fraudulently appear that the click and advertisement had originated from one of the Defendant's Publisher Networks, rather than from the search engine or the website on which the click or advertisement actually appeared.

32. The defendants and their co-conspirators caused advertising fees paid by ad brokers to the Defendants' Publisher Networks to be deposited into various bank accounts held in the name, or for the benefit, of the defendants, including accounts in Cyprus, Denmark and Estonia. The defendants used a portion of these funds to pay for the rental of the Rogue DNS Servers in New York and Chicago.

33. In furtherance of the scheme, the defendants and their co-conspirators controlled more than 1,000 IP addresses associated with the Rogue DNS Servers. However, to conceal their control and operation of the Rogue DNS Servers, the defendants registered the Rogue DNS Servers' IP addresses in the names of ProLite, Promnet, Internet Path, Cernel, and/or other entities with which the defendants had no public affiliation, but which they controlled. By using different entities to register IP addresses for the Rogue DNS Servers, the defendants furthermore concealed the

relationship between the Defendants' Publishing Networks and the Rogue DNS Servers.

STATUTORY ALLEGATIONS

34. From at least in or about 2007, up to and including in or about October 2011, in the Southern District of New York and elsewhere, VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit wire fraud in violation of Title 18, United States Code, Section 1343.

35. It was a part and an object of the conspiracy that VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, and others known and unknown, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343.

OVERT ACTS

36. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about October 23, 2007, ANTON IVANOV, the defendant, sent an email confirming ownership of IP addresses 85.255.112.0 to 85.255.127.255.

b. On or about August 11, 2008, VALERI ALEKSEJEV, the defendant, sent to VLADIMIR TSASTSIN, the defendant, an email (the "Email") containing a link to an online report about rogue DNS servers which identified several servers by their IP addresses; TSASTSIN commented in the email: "There are our IPs."

c. On or about August 11, 2008, TSASTSIN forwarded the Email to other co-conspirators not named as defendants herein, with the comment, "Read about us."

d. On or about August 15, 2008, after receiving a copy of the Email and in an apparent response to it, TIMUR GERASSIMENKO, the defendant, sent an email to DMITRI JEGOROV, the defendant, instructing JEGOROV to assign a new IP address to one of the servers identified in the online report referenced in the Email.

e. On or about August 15, 2008, in response to GERASSIMENKO's request, JEGOROV sent GERASSIMENKO an email containing a new IP address for the server.

f. On or about August 15, 2008, ANDREY TAAME, the defendant, sent an email to TSASTSIN asking if TSASTSIN intended to use a fake name for contracts with ad brokers.

g. On or about September 5, 2008, KONSTANTIN POLTEV, the defendant, sent an email to TSASTSIN inquiring if POLTEV should use fake information to register domain names.

h. On or about March 24, 2009, TSASTSIN sent an electronic message requesting technical assistance to the Manhattan Data Center.

(Title 18, United States Code, Section 1349.)

COUNT TWO

(Conspiracy to Commit Computer Intrusion)

The Grand Jury further charges:

37. The allegations in paragraphs 1 to 33 and 36 are repeated, realleged and incorporated by reference as though fully set forth herein.

38. From at least in or about 2007, up to and including in or about October 2011, in the Southern District of New York and elsewhere, VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and

with each other to violate Title 18, United States Code, Sections 1030(a)(4), (a)(5)(A) and (B), (c)(3)(A), and (c)(4)(A) and (B).

39. It was a part and an object of the conspiracy that VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, and others known and unknown, knowingly and with intent to defraud, would and did access a protected computer without authorization, and would and did exceed authorized access, and by means of such conduct would and did further the intended fraud and obtain anything of value, in violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A).

40. It was a further part and an object of the conspiracy that VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, and others known and unknown, knowingly and willfully would and did cause the transmission of a program, information, code, and command, and as a result of such conduct, would and did intentionally cause damage without authorization, to a protected computer, and would and did cause loss to one and more persons during any one-year period aggregating at least $5,000 in value, and would and did cause damage affecting 10 and more protected computers during any one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(B)(i) and (c)(4)(A)(I) and (VI).

41. It was a further part and an object of the conspiracy that VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, and others known and unknown, would and did intentionally access a protected computer without authorization, and as a result of such conduct, would and did recklessly cause damage, and would and did cause loss to one and more persons during any one-year period aggregating at least $5,000 in value, and would and did cause damage affecting 10 and more protected computers during any one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(B) and (c)(4)(A)(i)(I) and (VI).

OVERT ACTS

42. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about October 23, 2007, ANTON IVANOV, the defendant, sent an email confirming ownership of IP addresses 85.255.112.0 to 85.255.127.255.

b. On or about August 11, 2008, VALERI ALEKSEJEV, the defendant, sent to VLADIMIR TSASTSIN, the defendant, an email (the "Email") containing a link to an online report about rogue DNS servers which identified several servers by their IP addresses; TSASTSIN commented in the email: "There are our IPs."

c. On or about August 11, 2008, TSASTSIN forwarded the Email to other co-conspirators not named as defendants herein, with the comment, "Read about us."

d. On or about August 15, 2008, after receiving a copy of the Email and in an apparent response to it, TIMUR GERASSIMENKO, the defendant, sent an email to DMITRI JEGOROV, the defendant, instructing JEGOROV to assign a new IP address to one of the servers identified in the online report referenced in the Email.

e. On or about August 15, 2008, in response to GERASSIMENKO's request, JEGOROV sent GERASSIMENKO an email containing a new IP address for the server.

f. On or about August 15, 2008, ANDREY TAAME, the defendant, sent an email to TSASTSIN asking if TSASTSIN intended to use a fake name for contracts with ad brokers.

g. On or about September 5, 2008, KONSTANTIN POLTEV, the defendant, sent an email to TSASTSIN inquiring if POLTEV should use fake information to register domain names.

h. On or about March 24, 2009, TSASTSIN sent an electronic message requesting technical assistance to the Manhattan Data Center.

(Title 18, United States Code, Section 1030(b).)

COUNT THREE

(Wire Fraud)

The Grand Jury further charges:

43. The allegations of paragraphs 1 to 33 and 36 are repeated, realleged and incorporated by reference as though fully set forth herein.

44. From at least in or about 2007, up to and including in or about October 2011, in the Southern District of New York and elsewhere, VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, and others known and unknown, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations and promises, transmitted and caused to be transmitted, and attempted to transmit, by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, to wit, in furtherance of the Internet advertising fraud scheme described above in paragraphs 1 through 33, TSASTSIN, TAAME, GERASSIMENKO, JEGOROV, ALEKSEJEV, POLTEV, IVANOV and their co-conspirators caused malware to be distributed to computers world-wide through the Internet, and operated Rogue DNS Servers located in New York, New York and elsewhere

that received DNS queries and transmitted fraudulent DNS query results, over the Internet.

(Title 18, United States Code, Sections 1343 and 2.)

COUNT FOUR

(Computer Intrusion Furthering Fraud)

The Grand Jury further charges:

45. The allegations of paragraphs 1 to 33 and 36 are repeated, realleged and incorporated by reference as though fully set forth herein.

46. From at least in or about 2007, up to and including in or about October 2011, VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, and others known and unknown, knowingly and with intent to defraud, accessed a protected computer without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained anything of value, to wit, TSASTSIN, TAAME, GERASSIMENKO, JEGOROV, ALEKSEJEV, POLTEV, IVANOV and their co-conspirators caused malware to be distributed to computers world-wide through the Internet, and operated Rogue DNS Servers located in New York, New York, and elsewhere that received DNS queries from computers infected with the DNS Changer Malware, including NASA computers, and transmitted fraudulent DNS query results to those infected computers, in

furtherance of the advertising fraud scheme described above in paragraphs 1 to 33.

(Title 18, United States Code, Sections 1030(a)(4), 1030(c)(3)(A), and 2.)

COUNT FIVE

(Computer Intrusion by Transmitting Data)

The Grand Jury further charges:

47. The allegations of paragraphs 1 to 33 and 36 are repeated, realleged and incorporated by reference as though fully set forth herein.

48. From at least in or about 2007, up to and including in or about October 2011, VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, and others known and unknown, knowingly and willfully caused the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, and caused loss to one and more persons during any one-year period aggregating at least $5,000 in value, and caused damage affecting 10 and more protected computers during any one-year period, to wit, TSASTSIN, TAAME, GERASSIMENKO, JEGOROV, ALEKSEJEV, POLTEV, IVANOV and their co-conspirators caused malware to be distributed

to computers world-wide through the Internet and transmitted fraudulent DNS query results to computers infected with the DNS Changer Malware, including, but not limited to, more than 10 NASA computers thereby causing NASA damages in excess of $60,000.

(Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(A)(i)(I) and (VI), (c)(4)(B)(i), and 2.)

COUNT SIX

(Money Laundering - Promotion)

49. The allegations of paragraphs 1 to 33 and 36 are repeated, realleged and incorporated by reference as though fully set forth herein.

50. From at least in or about 2008, up to and in or about October 2011, in the Southern District of New York and elsewhere, VLADIMIR TSASTSIN, the defendant, in an offense affecting interstate and foreign commerce, transported, transmitted, and transferred, and attempted to transport, transmit, and transfer a monetary instrument and funds to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, to wit, to promote the wire fraud and computer intrusion offenses charged in Counts One through Five TSASTSIN caused money derived from those offenses to be sent (1) from an account he controlled in Estonia to the Manhattan Data Center's account at JPMorgan Chase Bank in New York, New York (the "Manhattan

Data Center-Chase Account"), (2) from the Furox-USD Account in Denmark to the account of a data center located in Chicago, Illinois (the "Chicago Data Center") maintained at the Bank of America in Virginia (the "Chicago Data Center-BofA Account"), and (3) from an advertising network in Canada to the Manhattan Data Center-Chase Account.

(Title 18, United States Code, Sections 1956(a)(2)(A) and 2.)

COUNTS SEVEN TO TWENTY-SEVEN

(Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity)

The Grand Jury further charges:

51. The allegations of paragraphs 1 to 33 and 36 are repeated, realleged and incorporated by reference as though fully set forth herein.

52. On or about the dates set forth below, in the Southern District of New York and elsewhere, VLADIMIR TSASTSIN, the defendant, willfully and knowingly engaged and attempted to engage in a monetary transaction, in and affecting interstate and foreign commerce, in criminally derived property of a value greater than $10,000 and which was derived from specified unlawful activity, namely, wire and computer-related frauds charged in Counts One through Five, to wit, TSASTSIN effected the following wire transfers involving proceeds derived from fraud:

COUNT	DATE	WIRE TRANSFERS FROM ACCOUNT IN THE NAME OF:	AMOUNT OF WIRE TRANSFER (USD)	TO ACCOUNT IN THE NAME OR FOR THE BENEFIT OF:
7	3/13/2009	Rove Digital	41,814.00	Chicago Data Center
8	4/3/2009	Rove Digital	25,060.71	Manhattan Data Center
9	5/5/2009	Rove Digital	17,397.20	Chicago Data Center
10	5/14/2009	Rove Digital	24,048.00	Manhattan Data Center
11	5/20/2009	Furox	750,000.00	Charles Schwab & Co.
12	6/5/2009	Rove Digital	11,346.00	Chicago Data Center
13	7/29/2009	Rove Digital	10,621.00	Chicago Data Center
14	9/18/2009	Rove Digital	23,646.00	Chicago Data Center
15	11/28/2009	Furox	780,000.00	Onwa (Cyprus)
16	1/20/2010	Furox	150,000.00	Onwa (Cyprus)
17	2/11/2010	Furox	160,000.00	Onwa (Cyprus)
18	3/11/2010	Furox	210,000.00	Onwa (Cyprus)
19	5/6/2010	Furox	500,000.00	Onwa (Cyprus)
20	6/2/2010	Furox	30,100.00	M.H.V.
21	6/28/2010	Furox	300,000.00	Onwa (Cyprus)
22	7/19/2010	Furox	120,000.00	Onwa (Cyprus)
23	9/7/2010	Furox	140,000.00	Onwa (Cyprus)
24	9/21/2010	Furox	100,000.00	Onwa (Cyprus)
25	12/14/2010	Furox	180,000.00	Onwa (Cyprus)
26	12/21/2010	Furox	33,332.58	Chicago Data Center
27	12/23/2010	Furox	91,000.00	Onwa (Cyprus)

(Title 18, United States Code, Sections 1957 and 2.)

FORFEITURE ALLEGATIONS AS TO COUNTS ONE AND THREE

53. As the result of committing one or more of the wire fraud and conspiracy offenses, in violation of Title 18, United States Code, Sections 1343 and 1349, alleged in Counts One and Three of this Indictment, VLADIMIR TSASTSIN, TIMUR GERASSIMENKO, VALERI ALEKSEJEV, DMITRI JEGOROV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, shall forfeit to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461, all property, real and personal, which constitutes and is derived from proceeds traceable to the offenses, including but not limited to the following:

a. At least $14,000,000 in United States currency, in that such sum in aggregate is property that represents or is traceable to the gross receipts obtained as a result of the wire fraud offenses;

b. Any and all United States currency, funds or other monetary instruments credited to the following accounts:

i. Nordea Bank Danmark A/S Account Nos. DK3520005036250625 and DK3520005036246059, in the name of Furox Aps;

ii. Bank of Cyprus Account No. CY27002001550000004061626106, for the benefit of Onwa Limited;

iii. Bank of Cyprus Account No. CY38002001550000004046807606, for the benefit of Lintor Limited;

iv. Bank of Cyprus Account Nos. CY66002001550000004081187006, CY72002001550000000113088200, and CY20002001550000004081188901, for the benefit of Danona Limited;

v. Marfin Popular Bank in Cyprus Account Nos. CY50003001680000016832019961 and CY08003001680000016811019441, for the benefit of Lex Capital Ltd;

vi. Marfin Popular Bank in Cyprus Account No. CY92003001790000017932264691, for the benefit of Onwa Limited;

vii. Interactive Brokers LLC in the United States Account Nos. U565997 and U595413, in the name of Lex Capital Limited;

viii. Sampo Bank in Estonia Account No. EE063300333436290009, in the name of Onwa Limited;

ix. Vorarlberger Landes in Austria, Account No. AT755800020497851018, for the benefit of Lintor Limited;

x. BMI Offshore Bank in the Republic of Seychelles Account No. 300000005588, in the name of Onwa Limited;

c. The defendants' interests in all computers and computer peripherals:

i. associated with IP addresses 85.255.112.0 through 85.255.127.255; 67.210.0.0 through 67.210.15.255; 93.188.160.0 through 93.188.167.255; 77.67.83.0 through 77.67.83.255; 213.109.64.0 through 213.109.79.255; 64.28.176.0

through 64.28.191.255; 69.197.132.58; 72.233.76.82; 174.123.205.190; 174.133.7.122; 184.82.214.2; 216.127.191.66; 64.20.51.2; 65.60.9.234; 65.60.9.235; 65.60.9.236; 65.60.9.237; 65.60.9.238; 66.152.177.58; 72.18.192.58; 72.18.192.59; 72.18.192.60; 72.18.192.61; 72.233.76.66; 72.233.76.67; 72.233.76.68; 72.233.76.69; 72.233.76.70; 65.254.36.122; 65.254.50.10; 72.9.238.202; 75.127.76.194; 207.210.119.170; 216.180.243.10; 64.111.197.186; 66.230.167.218; and 69.93.95.234 (the "TARGET IP ADDRESSES");

ii. located at the Manhattan Data Center;

iii. located at the Chicago Data Center;

iv. located at ThePlanet in Houston, Texas;

v. located at Multacom Corporation in Canyon County, California;

vi. located at Layered Technologies in Plano, Texas;

vii. located at Network Operations Center, Inc. in Scranton, Pennsylvania;

viii. located at Wholesale Internet in Kansas City, Missouri;

ix. located at SingleHop in Chicago, Illinois;

x. located at PremiaNet in Las Vegas, Nevada;

xi. located at Interserver in Secaucus, New

Jersey;

xii. located at ISPrime, LLC, in Weehawken, New Jersey; and

xiii. located at Global Net Access LLC, in Atlanta, Georgia; and

d. The defendants' interests in the TARGET IP ADDRESSES.

54. If any of the above-described forfeitable property, as a result of any act or omission of the defendants -

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property.

(Title 18, United States Code, Sections 981, 1343, 1349; Title 28, United States Code, Section 2461; and Title 21, United States Code, Section 853.)

FORFEITURE ALLEGATIONS AS TO COUNTS TWO, FOUR AND FIVE

55. As a result of committing one or more of the computer intrusion and conspiracy offenses, in violation of Title 18, United States Code, Section 1030, alleged in Counts Two, Four and Five, VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, VALERI ALEKSEJEV, DMITRI JEGOROV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2)(B), any property constituting, and derived from, proceeds obtained directly and indirectly as a result of the offenses, including but not limited to the following:

a. At least approximately $14 million in United States currency, in that such sum in aggregate is property representing the amount of proceeds obtained as a result of the offenses; and

b. Any and all United States currency, funds or other monetary instruments credited to the following accounts:

i. Nordea Bank Danmark A/S Account Nos. DK3520005036250625 and DK3520005036246059, in the name of Furox Aps;

ii. Bank of Cyprus Account No. CY27002001550000004061626106, for the benefit of Onwa Limited;

iii. Bank of Cyprus Account No. CY38002001550000004046807606, for the benefit of Lintor Limited;

iv. Bank of Cyprus Account Nos. CY66002001550000004081187006, CY72002001550000000113088200, and CY20002001550000004081188901, for the benefit of Danona Limited;

v. Marfin Popular Bank in Cyprus Account Nos. CY50003001680000016832019961 and CY08003001680000016811019441, for the benefit of Lex Capital Ltd;

vi. Marfin Popular Bank in Cyprus Account No. CY92003001790000017932264691, for the benefit of Onwa Limited;

vii. Interactive Brokers LLC in the United States Account Nos. U565997 and U595413, in the name of Lex Capital Limited;

viii. Sampo Bank in Estonia Account No. EE063300333436290009, in the name of Onwa Limited;

ix. Vorarlberger Landes in Austria, Account No. AT755800020497851018, for the benefit of Lintor Limited;

x. BMI Offshore Bank in the Republic of Seychelles Account No. 300000005588, in the name of Onwa Limited;

c. The defendants' interests in all computers and computer peripherals:

i. associated with the TARGET IP ADDRESSES;

ii. located at the Manhattan Data Center;

iii. located at the Chicago Data Center;

iv. located at ThePlanet in Houston, Texas;

v. located at Multacom Corporation in Canyon County, California;

vi. located at Layered Technologies in Plano, Texas;

vii. located at Network Operations Center, Inc. in Scranton, Pennsylvania;

viii. located at Wholesale Internet in Kansas City, Missouri;

ix. located at SingleHop in Chicago, Illinois;

x. located at PremiaNet in Las Vegas, Nevada;

xi. located at Interserver in Secaucus, New Jersey;

xii. located at ISPrime, LLC, in Weehawken, New Jersey; and

xiii. located at Global Net Access LLC, in Atlanta, Georgia; and

d. The defendants' interests in the TARGET IP ADDRESSES.

56. As a result of committing one or more of the computer intrusion and conspiracy offenses, in violation of Title 18, United States Code, Section 1030, alleged in Counts Two, Four and Five, VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, VALERI ALEKSEJEV, DMITRI JEGOROV, KONSTANTIN POLTEV, and ANTON IVANOV, the

defendants, shall forfeit to the United States, pursuant to 18 U.S.C. § 1030(i)(1), their interests in any personal property that was used and intended to be used to commit and to facilitate the commission of the offenses, including but not limited to the following:

a. The defendants' interests in all computers and computer peripherals:

i. associated with the TARGET IP ADDRESSES;

ii. located at the Manhattan Data Center;

iii. located at the Chicago Data Center;

iv. located at ThePlanet in Houston, Texas;

v. located at Multacom Corporation in Canyon County, California;

vi. located at Layered Technologies in Plano, Texas;

vii. located at Network Operations Center, Inc. in Scranton, Pennsylvania;

viii. located at Wholesale Internet in Kansas City, Missouri;

ix. located at SingleHop in Chicago, Illinois;

x. located at PremiaNet in Las Vegas, Nevada;

xi. located at Interserver in Secaucus, New Jersey;

xii. located at ISPrime, LLC, in Weehawken, New

Jersey; and

xiii. located at Global Net Access LLC, in Atlanta, Georgia; and

b. The defendants' interests in the TARGET IP ADDRESSES.

Substitute Assets Provision

57. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to 18 U.S.C. § 982(b), to seek forfeiture of any other property of the defendants up to the value of the above-described forfeitable property.

(Title 18, United States Code, Sections 982 and 1030, and Title 21, United States Code, Section 853.)

FORFEITURE ALLEGATIONS AS TO COUNTS SIX TO TWENTY-SEVEN

58. As a result of committing one or more of the money laundering offenses alleged in Counts Six to Twenty-Seven, VLADIMIR TSASTSIN, the defendant, shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(1), all property, real and personal, involved in such offense and all property traceable to such property, including but not limited to the following:

a. At least $14 million in United States currency, in that such sum in aggregate is property which was involved in the money laundering offense or is traceable to such property; and

b. Any and all United States currency, funds or other monetary instruments credited to the following accounts:

i. Nordea Bank Danmark A/S Account Nos. DK3520005036250625 and DK3520005036246059, in the name of Furox Aps;

ii. Bank of Cyprus Account No. CY27002001550000004061626106, for the benefit of Onwa Limited;

iii. Bank of Cyprus Account No. CY38002001550000004046807606, for the benefit of Lintor Limited;

iv. Bank of Cyprus Account Nos. CY66002001550000004081187006, CY72002001550000000113088200, and CY20002001550000004081188901, for the benefit of Danona Limited;

v. Marfin Popular Bank in Cyprus Account Nos. CY50003001680000016832019961 and CY08003001680000016811019441, for the benefit of Lex Capital Ltd;

vi. Marfin Popular Bank in Cyprus Account No. CY92003001790000017932264691, for the benefit of Onwa Limited;

vii. Interactive Brokers LLC in the United States Account Nos. U565997 and U595413, in the name of Lex Capital Limited;

viii. Sampo Bank in Estonia Account No. EE063300333436290009, in the name of Onwa Limited;

ix. Vorarlberger Landes in Austria, Account No. AT755800020497851018, for the benefit of Lintor Limited;

x. BMI Offshore Bank in the Republic of Seychelles Account No. 300000005588, in the name of Onwa Limited;

c. The defendants' interests in all computers and computer peripherals:

i. associated with the TARGET IP ADDRESSES;

ii. located at the Manhattan Data Center;

iii. located at the Chicago Data Center;

iv. located at ThePlanet in Houston, Texas;

v. located at Multacom Corporation in Canyon County, California;

vi. located at Layered Technologies in Plano,

Texas;

vii. located at Network Operations Center, Inc. in Scranton, Pennsylvania;

viii. located at Wholesale Internet in Kansas City, Missouri;

ix. located at SingleHop in Chicago, Illinois;

x. located at PremiaNet in Las Vegas, Nevada;

xi. located at Interserver in Secaucus, New Jersey;

xii. located at ISPrime, LLC, in Weehawken, New Jersey; and

xiii. located at Global Net Access LLC, in Atlanta, Georgia; and

d. The defendants' interests in the TARGET IP ADDRESSES.

Substitute Assets Provision

59. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to 18 U.S.C. § 982(b), to seek forfeiture of any other property of said defendant up to the value of the above-described forfeitable property.

(Title 18, United States Code, Sections 982, 1956 and 1957, and Title 21, United States Code, Section 853.)

Foreperson

PREET BHARARA
United States Attorney